International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN(P): 2249-684X; ISSN(E): 2249-7951
Vol. 5, Issue 3, Jun 2015, 77-80
© TJPRC Pvt. Ltd.

CUSTOMIZED PROGRAMMABLE INTERFACE FOR AUTHENTICATED ENCRYPTION

RUDRAGOUDA MUKARTIHAL[1], RAHUL M PATIL[2]
VIJAYKUMAR SAJJANAR[3] & SHRIKANT PUROHIT[4]

[1]Department of Electronics and Communication Engineering, BLDEA's VP DrPGH CET, Vijayapur, Karnataka, India

[2]Application Developer, Department of Electronics and Communication Engineering, BLDEA's VP DrPGH CET, Vijayapur, Karnataka, India

[3]Department of Electronics and Communication Engineering, BLDEA's VP DrPGH CET, Vijayapur, Karnataka, India

[4]Department of Electronics and Communication Engineering, BLDEA's VP DrPGH CET, Vijayapur, Karnataka, India

ABSTRACT

The widespread usage of social networking in personal and professional fields has increased the concern of security and integrity of information. This paper provides a solution on pre-network level through authenticated encryption and hence increasing the confidence in posting and sharing data on internet or cloud. Graphical user interfaces on the end users' level for authenticating and encrypting data serve as a powerful tool in adressing data security attacks.

KEYWORDS: Encryption, Authentication, User Interface, Security

INTRODUCTION

Authentication and encryption are key tasks in communication provided by various network layers. This paper demonstrates customized and personalised interface for secured digital communication. The increased embeddment of internet and social networks in society has made personal information easily exposed and abused [1]. Information collected by operators and third parties is identified as a significant security concern [1]. User's privacy is jeopardized by companies with exploit of harvested information for various purposes [1].Authentication and encryption when carried out seperately on data leads to processing twice.Authenticated encryption is a way to bring about single functionality and fast processing of big data sizes [2].

Several methods in the form of easy softwares and applications are available for authentication and encryption of data. These tools follow a strict procedure and code for obtaining the end results. The proposed graphical user interfaces (GUI) provide a platform for users to customize the method of authenticated encryption on designs.

USER INTERFACES

Pre Network Level

Information is secured and transeived on the internet by utilising the UI shown in figure.1 The data is processed for authentication and encryption by simple user tools mentioned in section III. The data is then a garbage waste for any looker online without an idea of what coding has been employed. The solutions available for information security like operator

solutions, commercial solutions or academic solutions [1] are products of general awareness and publicised application products are prone to be obsolete with time. The designed PIs provide a solution to these owes. The encryption and authentication schemes for multimedia and text are different [3].The PI (Programmable Interface) designed are openly variable to work for all types of information. As observed in the results of section III the data moving online is non-interprettable as text or multimedia or instructions.

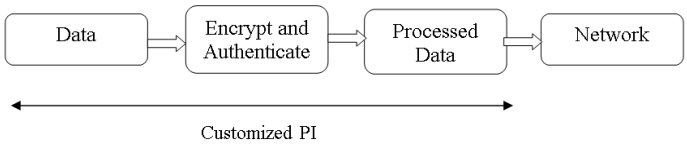


Figure 1: Pre-Network PI Model

PI for Computer System

As of 2014, the number of internet users worldwide was 2.92 billion, up from 2.71 billion in the previous year [4]. Computer systems are often opted for communication of large data over internet. The PI hence designed incurrs less delay and easily manipulatable for the level of encryption required.

PI for Samrtphones

The number of smartphone users worldwide will surpass 2 billion in 2016, according to new figures from eMarketer—after nearly getting there in 2015. Next year, there will be over 1.91 billion smartphone users across the globe, a figure that will increase another 12.6% to near 2.16 billion in 2016 [5]. The advent of smartphones into people's lives brought varous challenges in managing data and its security. The PI designed for smartphones need to have ability for ease of usage. The PI further has various frendly ways of obtaining data through microphone and communication of secured data with one touch SMS(Short Message Service) and email.

DESIGN AND RESULT

The PI designed for computer system is for a general processor corei7 2.5GHz with RAM 8GB. The operating system is windows 8.1 The designed PI is by Matlab R2012a.

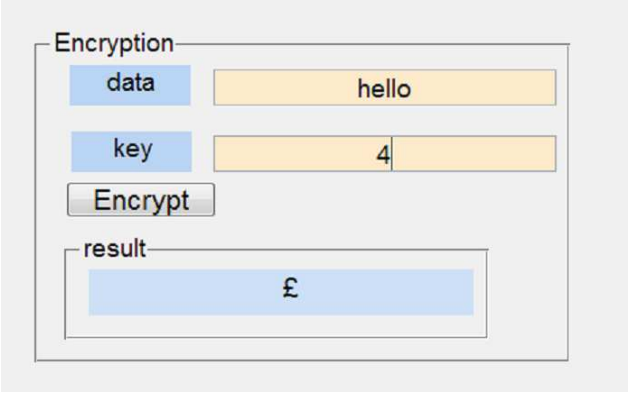
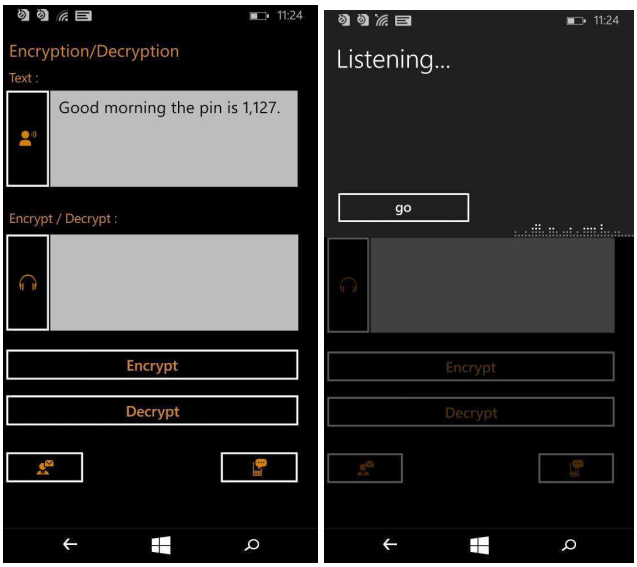


Figure 2: PI Developed For Computer Systems, Transmitter Side

The PI designed for smart phone is for an embedded processor Qualcomm Snapdragon 400, 1.2GHz with 512MB RAM. The operating system is Microsoft Windows phone 8.1. The designed PI is by Microsoft Visual studio. The screenshots are from smartphone Microsoft Lumia 635.



(a) **(b)**

Figure 3: (a) Developed PI For Smartphone (b) PI Indicating Reading of Data through Microphone

Table 1: Design Results

	Input Raw Data	Output Pi Data
Smartphone	Hello world	yxeNnZSoxM/xWTToZo18uEQv1B2wONp52EOV/7/KqhN8=
	Good morning	rdqDIRQJajjQB xGK4lVnjUj98f47Q7SdCcVNLGAYvM=
Computer System	Hello world	r458459unfgngkmvjn[]=-0\
	Good morning	23yut785nhj'[]-=098nm\\[

Table 1 shows the authenticated and encrypted data by smartphone and computer systems for two randomn messages. The resulting data are by customized simple matrix variations of raw text. The processsed data can then be safely communicated to limited group of people who have the information of the processing done. The processing methods can be manipulated during authentication for increased data security.

CONCLUSIONS

The designs and results show advantages of having a personalized interface(PI) for authenticated encryption. Masking of data as garbage provides a high level of security against online threats. The PIs provide a secure and confident way to transmit critical and confidential data online/on cloud. The designs can further be improved to combine available sophisticated encryption and authentication standards with the users' methods.

REFERENCES

1. "Online Social Networks: Threats and Solutions", Michael Fire, Roy Goldschmidt, and Yuval Elovici. IEEE COMMUNICATION SURVEYS & TUTORIALS 2014.

2. "Authenticated Encryption: Toward Next-Generation Algorithms", Diana Maimut, Reza Reyhanitabar , IEEE Computer and Reliability Societies, March/April 2014
3. "Towards the Growth of Image Encryption andAuthentication Schemes"Amitesh Singh Rajput, Nishchol Mishra, Sanjeev Sharma, International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2013
4. Global number of worldwide internet users , www.statista.com/statistics/273018/number-of-internet-users-worldwide/
5. 2 Billion Consumers Worldwide to Get Smart(phones) by 2016, www.emarketer.com/
6. Microsoft Visual studio, https://www.visualstudio.com/
7. Matworks, http://in.mathworks.com/